U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.255
May 15, 1999

DEPARTMENTAL GUIDE TO INCIDENT HANDLING PLANNING

TABLE OF CONTENTS

DEPARTMENTAL GUIDE
TO
INCIDENT HANDLING PLANNING

1. PURPOSE

The purpose of this Guide is to provide Department of Transportation (DOT) and their Operating Administration managers, ISSO's and network administrators with a step-by-step approach for developing an Incident Handling capability within their organizations, and Incident Response Teams capable of responding effectively and efficiently to information system security "incidents".

2. SCOPE

The provisions of this Guide apply to the Department of Transportation (DOT), its Secretarial Offices and Operating Administrations.

3. GOALS

The Goal of incident handling planning is to provide reasonable methods for limiting the possibility of an adverse effect on a DOT Information System due to the occurrence of an information system security incident, and for facilitating the rapid and successful investigation of an incident, should one occur.

4. REFERENCES

The DOT Departmental Information Resources Management Manual (DIRMM) DOT H 1350.2 implements statutory and regulatory Information Resources Management (IRM) and security requirements for the Department. It also calls for ensuring the confidentiality, integrity, and availability of information contained, processed, or transmitted in/on sensitive systems. Refer to DOT H 1350.2.1 REGULATORY AND GUIDANCE DOCUMENTS for specific references.

5. OVERVIEW OF INCIDENT HANDLING

An information system security incident is an event that has actual—or the potential for—adverse effects on computer or network operations. Such incidents can result in fraud, waste, or abuse; can compromise information; or can cause loss or damage to property or information. An incident can result from a computer virus, other malicious code, employee malfeasance, or a system intruder, either an insider or an outsider. Although it is known that hackers and malicious code can pose serious threats to systems and networks, actual incidents of such damage cannot be predicted. Security incidents, such as break-ins and service disruptions, on larger networks (e.g., the Internet), have harmed the computing capabilities or various organizations.

Incident handling is closely related to Continuity Of Operations planning, as described in DOT H 1350.254 *Developmental Guide To Continuity Of Operations Planning*. In fact, an incident handling capability may be viewed as a component of Continuity Of Operations planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, Continuity Of Operations planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

When left unchecked, malicious software can significantly harm an organization's computing, depending on the technology and its connectivity. An incident handling capability provides a way for users to report incidents, and the appropriate response and assistance to be provided to aid in recovery. Technical capabilities (e.g., trained personnel, intrusion detection, and virus identification software) are prepositioned, ready to be used as necessary. Moreover, the organization will have already made important contacts with other supportive sources (e.g., legal, technical, and managerial) to aid in containment, identification and recovery efforts.

Like most Federal Agencies, DOT uses large LANs internally and also connects to public networks, such as the Internet. By doing so, DOT increases its exposure to threats from intruder activity. An incident handling capability can provide enormous benefits by allowing a rapid response to suspicious activity and coordinating incident handling with responsible agencies, offices and individuals, as necessary. Intruder activity, whether hackers or malicious code, can often affect many systems located at many different network sites; thus, handling the incidents can be logistically complex and can require information from outside the organization. By planning ahead, such contacts can be pre-established, and the speed of response improved, thereby containing and minimizing damage.

An incident handling capability also assists DOT in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally to gain a better understanding of current threats and vulnerabilities, so that more effective safeguards can be implemented. Additionally, through outside contacts (established by the incident handling capability) early warnings of threats and vulnerabilities can be provided. Mechanisms will already be in place to warn users of these risks.

Finally, having an incident handling capability allows DOT organizations to learn from the incidents that they have experienced. Data about past incidents (and the corrective measures taken) can be collected and analyzed for patterns. Vulnerabilities can also be identified via this process. Knowledge about the types of threats that are occurring and the presence of vulnerabilities can aid in identifying security solutions. This information will also prove useful in creating a more effective training and awareness program, and thus help reduce the potential for losses.

6. INFORMATION SYSTEM SECURITY INCIDENTS

A. Intrusion

This is the deliberate attempt by an individual (insider / outsider) to gain unauthorized access into a system. Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage media by obtaining superuser privileges. Unauthorized access could also entail access to network data by planting an unauthorized "sniffer" program or device to capture all packets traversing the network at a particular point.

B. Malicious Code

Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can furthermore replicate rapidly, thereby making containment an especially difficult problem.

C. Fraud and Theft

Information systems can be exploited for fraud and theft both by automating traditional methods of fraud and by using new methods. Systems that control access to any resource are targets (e.g., time and attendance systems, financial systems, inventory systems, and long-distance telephone systems). Information system fraud and theft can be committed by insiders or outsiders. Insiders are responsible for most incidents of fraud.

D. Errors and Omissions

Errors and omissions can be caused during the creation or modification of data.

E. Employee Sabotage and Abuse

Employees are most familiar with their employer's information systems and know which actions might cause the most damage, mischief, or sabotage. Common examples of information system-related sabotage include:

(1) Destroying hardware or facilities.

(2) Planting logic bombs that destroy programs or data.

(3) Intentionally entering data incorrectly.

(4) Crashing systems.

(5) Intentionally deleting data.

(6) Intentionally changing data.

F. Loss, Theft, or Damage

Computer equipment, software, and data may be misplaced, stolen, or physically damaged.

G. Denial of Service

The information system is not available for use to authorized personnel due to deliberate or accidental interference with system operations. Perpetrators and malicious code can disrupt system services in many ways, including erasing a critical program, "mail spamming" (flooding a user account with electronic mail), and altering system functionality by installing a Trojan horse program.

7. INCIDENT HANDLING PLANNING

Incident handling planning may be accomplished as a five-step process, consisting of:

Step 1 – Identifying measures that help to *prevent* incidents from occurring, such as the use of anti-virus software, firewalls, and other tools and practices.

Step 2 – Defining measures that can *detect* the occurrence of an incident, such as intrusion detection monitoring systems, firewalls, router tables and anti-virus software.

Step 3 – Establishing procedures for *reporting and communicating* an incident. This reporting procedure should notify all affected parties should an incident be detected, including parties both within and external to the affected organization.

Step 4 – Defining processes and measures for *responding* to a detected incident, in order to minimize damage, isolate the problem, resolve it, and restore the affected system(s) to normal operation. This also includes the creation of a Computer Security Incident Response Team (CSIRT) trained and responsible for incident response.

Step 5 – Developing a procedure for identifying and implementing *lessons learned* regarding the incident.

A Template for a Security Incident Handling Plan is contained in Attachment A of this Guide.

A. Incident Prevention

Preventing security incidents from occurring is a primary objective of the entire security planning process. The operational and technical controls emplaced as part of the Risk Management process, and detailed in the Information System Security Plan are designed to prevent the occurrence of the types of incidents described in Section 6 above. Refer to DOT H 1350.251

Departmental Guide to Developing an Information System Security Plan for more details on operational and technical controls for incident prevention.

B. Incident Detection

If an organization is not adequately prepared to detect the signs that an incident has occurred, is occurring, or is about to occur, it may be difficult or impossible to later determine if the organization's information system(s) have been compromised. Failure to identify the occurrence of an incident can leave the organization vulnerable in a number of ways:

- Damage to data, systems and networks due to not taking timely action to contain and control an incident, resulting in loss of productivity, increased costs, etc.
- Damage affecting multiple systems both inside and outside of the organization due to an inability to react in time to prevent the spread of the incident.
- Negative exposure that can damage the organization's reputation and stature.
- Possible legal liability for failing to exercise an adequate standard of due care when the organization's information system(s) is used to inadvertently or intentionally "attack" other organizations.

(1) System and Network Logging Functions

Collecting data generated by system, network, application and user activities is essential for analyzing the security of these assets, and for incident detection. Log files contain information about what activities have occurred over time on the system. These files are often the only record of suspicious behavior, and may be used not only to detect an incident, but also to help with system recovery, aid in investigation, serve as evidence, and back up insurance claims. Incident detection planning should include identifying the types of logs and logging mechanisms available for each system asset, and the data recorded within each log. If vendor-provided logging mechanisms are insufficient to capture the data required, they should be supplemented with tools that capture the additional information. Logging functions should always be enabled.

(2) Detection Tools

It is important to supplement system and network logs with additional tools that watch for signs that an incident has occurred, or has been attempted. These include tools that monitor and inspect system resource use, network traffic and connections, and user account and file access; tools that scan for viruses; tools that verify file and data integrity; tools to probe for system and network vulnerabilities; and tools to reduce, scan, monitor and inspect log files. Examples of detection tools include:

- Tools that report system events, such as password cracking, or the execution of unauthorized programs.
- Tools that report network events, such as access during non-business hours, or the use of Internet Relay Chat (IRC), a common means of communication used by intruders.
- Tools that report user-related events, such as repeated login attempts, or unauthorized attempts to access restricted information.
- Tools that verify data, file and software integrity, including unexpected changes to the protections of files, or improperly set access control lists on system tools.
- Tools that examine systems in detail on a periodic basis, to check log file consistency or known vulnerabilities.

(3) Detection Techniques

The general approach for incident detection is based on three simple steps, --- observe/monitor information systems for signs of unusual activity, investigate anything thought to be unusual, and if something is found that cannot be explained by authorized activity, immediately initiate predetermined incident response procedures.

Recommended practices include:

- Ensuring that the software used to examine systems has not been compromised
- Looking for unexpected changes to directories or files
- Inspecting system and network logs
- Reviewing notifications from system and network monitoring mechanisms
- Inspecting processes for unexpected behavior
- Investigating unauthorized hardware attached to the organization’s network
- Looking for signs of unauthorized access to physical resources
- Reviewing reports by users and external contacts about suspicious system and network events and behavior

C. Incident Reporting and Communication

Designated organization personnel, as well as personnel outside of the organization cannot execute their responsibilities if they are not notified in a timely manner that an incident is occurring or has occurred, and if they are not kept informed as the incident progresses. In addition, there are types of incidents wherein the public communications aspects, if mishandled, could result in serious negative publicity or loss of reputation. Hence it is important that incident reporting and information dissemination procedures be established and periodically reinforced, so that all personnel are aware of how they are to participate when an incident occurs.

(1) Incident Reporting

Incident handling planning should specify who should be notified in the event of an intrusion, who does the notifying of whom, and in what order. The order of notification may depend on the type of incident, or on other circumstance. Parties to be notified include: (NOTE: These are not identified in any specific order)

- The Information Systems Security Officer (ISSO)
- The CSIRT, if one exists
- Public Relations
- System and Network Administrators
- Responsible Senior Management
- Human Resources
- Legal Counsel
- Law Enforcement Groups
- System/Network Users
- Other CSIRTS outside of the organization and/or DOT

(2) Communication

Communication aspects include:

- Defining specific roles and responsibilities for each contact within the organization, including their range of authority.

- Specifying how much information should be shared with each class of contact, and whether or not sensitive information needs to be removed or filtered prior to sharing it.
- Identifying who to notify and when to notify them by using specified communication mechanisms (e.g., phone, e-mail, fax, pager, etc.), and whether or not these mechanisms need to be secure.
- Identifying who has the authority to initiate information disclosure beyond that specified in DOT policy.

D. Incident Response

Planning for incident response should include the collection and protection of all relevant information, containing the incident, correcting the root problem leading to the incident, and, finally, returning the system to normal operation.

(1) Collect/Protect Information

All information regarding an information system security incident should be captured and securely stored. This may include system and network log files, network message traffic, user files, intrusion detection tool results, analysis results, system administrator logs and notes, backup tapes, etc. In particular, if the incident leads to a prosecution, such as for an intruder/hacker, disgruntled employee or a thief, it is necessary to have complete, thorough and convincing evidence that has been protected through a verifiable and secure chain-of-custody procedure. In order to achieve this level of information protection and accountability, it is necessary that:

- All evidence is accounted for at all times
- The passage of evidence from one party to the next is fully documented
- The passage of evidence from one location to the next is fully documented

Ensure that all critical information is duplicated and preserved both onsite and offsite in a secure location.

(2) Contain The Incident

Containment consists of short-term, tactical actions whose purpose it is to remove access to compromised systems, limit the extent of current damage to the system, and prevent additional damage from occurring. The specific steps to be followed depend upon the type of incident (intrusion, virus, theft, etc.), and whether the incident is ongoing (e.g., an intrusion) or is over (e.g., a theft of equipment). Considerations in planning for containment include:

- Defining the acceptable level of risk to business processes and the systems and networks that support them, and to what extent these processes, systems and networks must remain operational, even during a major security incident
- Methods for performing a rapid, overall assessment of the situation as it currently exists (scope, impact, damage, etc.)
- Determining whether to quickly inform users that an incident has occurred, or is occurring, that could affect their ability to continue work
- Identifying the extent to which containment actions might destroy or mask information required to later assess the cause of the incident
- If the incident is ongoing, identifying the extent to which containment actions might alert the perpetrator (e.g., an intruder, thief or other individual with malicious intent)
- Determining the applicability of existing Continuity Of Operations Planning (refer to DOT H 1350.254 *Departmental Guide to Continuity Of Operations Planning*)

- Identifying when to involve senior management in containment decisions, especially when containment includes shutting systems down or disconnecting them from a network
- Identifying who has the authority to make decisions in situations not covered by existing containment policy

Containment strategies include temporarily shutting down a system, disconnecting it from a network, disabling system services, changing passwords, disabling accounts, changing physical access mechanisms, etc. Specific strategies should be developed for serious incidents, such as:

- Denial of service due to e-mail "spamming" (sending a large volume of electronic messages to a targeted recipient) or "flooding" (filling a channel with garbage, thereby denying others the ability to communicate across it)
- Programmed threats, such as new viruses not yet detected and eliminated by anti-virus software, or malicious applets, such as those using ActiveX or Java
- The scanning, probing or mapping of systems by intruders planning on future system hacking attempts
- Major password compromises (e.g., an intruder with a password sniffer tool), requiring the need to change all user or account passwords at a specific site or at a specific organizational level

In general, the containment objective should be to provide a reasonable security solution until sufficient information has been gathered to take more appropriate actions to address the vulnerabilities exploited during the incident.

(3) Correct The Root Problem

Elimination of the root cause of a security incident oftentimes requires a great deal of analysis, followed by specific corrective actions, such as the improvement of detection mechanisms, changes in reporting procedures, enhanced protection mechanisms (such as firewalls), more sophisticated physical access controls, improved awareness and training, or specific changes to security policy and procedures.

(4) Return To Normal Operation

Restoring a compromised information system, and returning it to normal operation should ideally be accomplished only after the root cause of the incident has been corrected. Doing so prevents the same or similar type of incident from occurring again, or at least ensures that a recurring incident will be detected in a more timely fashion. However, business reality may require that the system may have to be restored to operation before a full analysis can be conducted, and all corrections made. Such a risk needs to be carefully managed and monitored, recognizing that the system remains vulnerable to another occurrence of the same type of incident. Thus an important part of the incident handling planning process is determining the requirements and timeframe for returning specific information systems to normal operation. The determination to return a system to normal operation prior to fully resolving the root problem should require the involvement of senior management.

Restoration steps include:

- Using the latest trusted backup to restore user data. Users should review all restored data files to ensure that they have not been affected by the incident.
- Enabling system and application services. Only those services actually required by the users of the system should be enabled initially.

- Reconnecting the restored system to its local area network. Validate the system by executing a known series of tests, where prior test results are available for comparison.
- Being alert for problem recurrence. A recurrence of a viral or intrusion attack is a real possibility. Once a system has been compromised, especially by an intruder, the system will likely become a target for future attacks.

E. Lessons Learned

It is important to learn from the successful and unsuccessful actions taken in response to security incidents. Capturing and disseminating what worked well and what did not will help to reduce the possibility for similar incidents, and thus improve the overall information system security posture of DOT. Otherwise, DOT systems and applications will continue to operate at risk, and will likely fall victim to the same or similar type of incident again. Establishing a lessons learned capability includes the following steps:

(1) Post Mortem Analysis

A post mortem analysis and review meeting should be held within three to five days of the completion of the incident investigation. Waiting too long could result in people forgetting critical information. Questions to be asked include:

- Did detection and response procedures work as intended? If not, why not?
- Are there any additional procedures that would have improved the ability to detect the incident?
- What improvements to existing procedures and/or tools would have aided in the response process?
- What improvements would have enhanced the ability to contain the incident?
- What correction procedures would have improved the effectiveness of the recovery process?
- What updates to policies and procedures would have allowed the response and/or recovery processes to operate more smoothly?
- How could user and/or system administrator preparedness be improved?
- How could communication throughout the detection and response processes be improved?

The results of these and similar questions should be incorporated into a report for senior management review/comment.

(2) Lessons Learned Implementation

As applicable, new and/or improved methods resulting from lessons learned should be included within current security plans, policies and procedures. In addition, there are public, legal and vendor information sources that should be periodically reviewed regarding intruder trends, new virus strains, new attack scenarios and new tools that could improve the effectiveness of DOT response processes.

(3) Risk Assessment

If the severity or impact of the incident was severe, a new risk assessment for the affected information system should be considered. Refer to DOT H 1350.252 *Departmental Guide to Risk Assessments* for additional guidance.

8. COMPUTER SECURITY INCIDENT RESPONSE TEAM

A Computer Security Incident Response Team (CSIRT), oftentimes shortened to Computer Incident Response Team (CIRT) is a group of professionals within the organization, who are trained and chartered to respond to a serious security incident. The CSIRT has both an investigative and a problem-solving component, and should include management personnel with the authority to act, technical personnel with the knowledge and expertise to rapidly diagnose and resolve problems, and communications personnel able to keep the appropriate individuals and organizations properly informed as to the status of the problem, and develop public image/crisis control strategies, as necessary.

The composition of the CSIRT, and the circumstances under which it is activated must be clearly defined, in advance, as part of the incident handling planning process. The Team should be available and on call in emergency situations, and possess the authority to make decisions in real time. Procedures that define the circumstances under which the CSIRT is activated must be clear and unambiguous. Activation for every simple incident, such as an employee's data entry error, can be wasteful and time-consuming. On the other hand, if a serious incident, such as an intrusion attack, is in progress, then delaying the activation of the Team could result in serious damage to the organization. Activation should therefore be considered only when information systems must be protected against serious compromise, --- an unexpected, unplanned situation that requires immediate, extraordinary and fast action to prevent a serious loss of organizational assets and/or mission capability. The individual within the organization authorized to activate the CSIRT should also be clearly identified.

The planning process should also consider which Team members will be needed for different kinds and levels of incidents, and how they are to be contacted when an emergency occurs. Finally, the members of the CSIRT need to be adequately trained to handle their duties rapidly and effectively. Training should include both the procedures to be followed in responding to a serious security incident, and the specific technical skills that individual Team members might require in order to adequately perform their assigned tasks. Periodic simulations of security incidents should be considered, as an additional method for maintaining Team effectiveness.

ATTACHMENT A

SECURITY INCIDENT HANDLING PLAN TEMPLATE

[TO BE SUPPLIED]